Notice of Allowability	**Application No.** 09/758,941	**Applicant(s)** RYGAARD, CHRISTOPHER A.	
	Examiner Jenise E Jackson	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to _3/1/05_.

2. ☒ The allowed claim(s) is/are _1-8 and 15-30_.

3. □ The drawings filed on _____ are accepted by the Examiner.

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 03142005.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _03142005_ .
7. □ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner's Statement

1. Formal Drawings are required; the drawings need to be submitted to the Draftsperson, pursuant to the allowability of this application.

Reasons For Allowance

1. The status of claims: previous office action, dated June 21, 2004 the Examiner indicated that claims 9-14 and claims 15-16 were allowable but were objected to because base claims were rejected. The Applicant has amended claims 1-8, and 15-16, and has added claims 17-30 which contain allowable subject matter. Claims 9-14 are canceled. The reasons that Claims 1-8, 15-30 are listed below:

2. In the prior art of file protection, prior art fails to disclose or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted". An example of prior art that fails to disclose or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", "stripping the code from the mobile application when the code is

marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe" , is Walsh. Walsh discloses an agent includes a mobile object, which can travel from a first computer to a second computer in a computer network. The agent is generated and stored in memory on the first computer and then migrates to the second computer by being transmitted across the network. When the agent of Walsh completes execution on the second computer, the agent acts in accordance to the agent itinerary. Walsh also allows each agent to be able to change its itinerary. This is in direct contrast to the claims, which calls for, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe". There is no monitoring being performed in Walsh. Security is not even discussed or suggested. The agent is able to change its own itinerary, which is in direct contrast to claim limitations above. Thus, prior art fails to suggest or disclose the limitations above.

3. Another example in the prior art of file protection, that fails to disclose or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if

code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted", is Heddaya. Heddaya et al. discloses the mobile agent instructs the intermediate node to operate as a front-end server by executing code of the mobile agent such that the intermediate node provides at least a portion of the requested service. The mobile agent instructs the node to inspect network traffic and operate either as a secondary server node of the mobile agent. In contrast to prior art of file protection, the claims are not disclosed or suggested in prior art, the claims disclose, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted". The agents of Heddaya do not disclose or suggest how the agents to chose where they are transferred. Thus, prior art of file protection fails to disclose the limitations above.

4. In the prior art of security, prior art fails to disclose or suggest, “monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe”, and “means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe”, and “stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted”; and example of prior art that fails to disclose or suggest, the limitations above is, Golan. Golan discloses creating a sandbox within which a plurality of downloaded software components can execute in a secure manner. The software executes within the sandbox. Prior art of security is in contrast to claims, which call for, monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe”, and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe”, and “stripping the code from the mobile application when the code

is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted".

5. In the prior art of networking, prior art fails to disclose or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted" . An example of prior art in networking that fails to disclose or suggest the limitation above, is Frew. Frew discloses a user wishing to transmit an intelligent mobile agent with appended information, such as the expert system mentioned above an example, then encodes the information using compression algorithms, and applies this in the form of a token. The token of Frew is used to perform task of the agent. The token is not used for security purposes or a means of monitoring. In contrast to prior art of networking, prior art fails to disclose or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable

itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted".

6. In the prior art of non-patent literature, prior art fails to teach or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted"; and example of non-patent literature that fails to teach or suggest the limitations above is, Jansen. Jansen teaches that a mobile agent has a prescribed security policy, and the policy can be included in a certificate. Jansen teaches that the agent moving among the platforms carries its certificate. The platform receiving the agent determines the relevancy of the agent's certificate. First, this in is direct contrast to claim limitations above, because each agent is not secure. The agent that travels to each platform of Jansen checks the certificate, not the central computer of the claim limitations. Furthermore, Jansen does not teach or suggest, monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code

known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted". If the certificate of Jansen is not valid that agent is not allowed to execute. Non-patent literature, and more specifically Jansen fails to teach, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted" .

7. Another example of non-patent literature that fails to teach or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted", is

Wong et al. Wong et al. teaches an agent roaming the network carries its own identity. At each stop in its travels, the agent's identity is verified against a list of the system's valid users. Each server includes a list of users as well as the corresponding resource-access permissions allowed for that user. Wong et al. also teaches that a digital signature can be associated with the agent to insures that the agent has not been altered. However, non-patent literature, fails to teach or suggest, "monitoring means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, and means for replacing the immutable code with code known by the central computer to be safe", and "means for monitoring includes means for inspecting an access control list of the mobile application to determine if the itinerary data of the mobile application is marked as immutable, and means for replacing the immutable itinerary data with itinerary data that is known by the central computer to be safe", and "stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

March 15, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100